PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-152587
(43)Date of publication of application : 31.05.1994

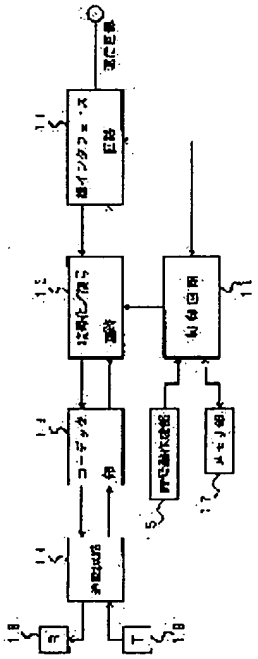
(51)Int.Cl. H04L 9/06
H04L 9/14

(21)Application number : 04-295766
(22)Date of filing : 05.11.1992

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MATSUZAWA HIROYUKI
KABETANI KIYOSHI

(54) METHOD AND DEVICE FOR DIGITAL COMMUNICATION

(57)Abstract:
PURPOSE: To provide a method and device for digital communication capable of changing communication cryptographic keys between communication terminal for each communication.
CONSTITUTION: When starting the communication, a cryptographic key preparing section 15 automatically generates a communication cryptographic key, which is ciphered by a ciphering/deciphering circuit 12 by means of a communication cryptographic key decoding key stored in a memory section 17. This is sent to a reception side through a network interface circuit 11. At the side of reception, the received ciphered communication cryptographic key is decoded by the circuit 12 by means of the communication cryptographic key decoding key. Then, the ciphered and decoded digital information is communicated by means of the communication cryptographic key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平6－152587
(43)公開日　平成6年(1994)5月31日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/06 9/14		7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　未請求　請求項の数３（全　６　頁）

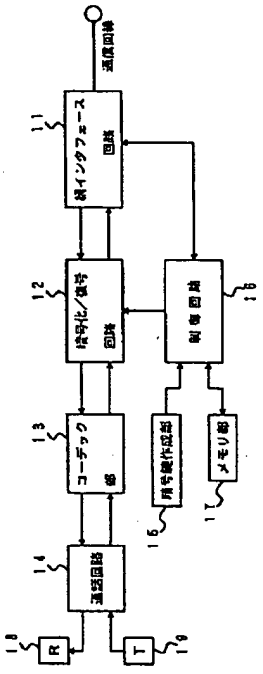
(21)出願番号　特願平4－295766

(22)出願日　平成４年(1992)11月５日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　松沢　裕之
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　壁谷　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　吉田　精孝

(54)【発明の名称】　ディジタル通信方法及びその装置

(57)【要約】
【目的】　通信端末同士で通信毎に通信用暗号鍵を変更可能なディジタル通信方法及びその装置を提供する。
【構成】　通信の開始時に、暗号鍵作成部１５により通信用暗号鍵を自動的に生成し、これをメモリ部１７に記憶された通信用暗号鍵解読鍵を用いて暗号化／復号回路１２により暗号化し、これを網インタフェース回路１１を通して受信側へ送信し、受信側では、該受信した前記暗号化された通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて暗号化／復号回路１２により復号化し、以後、該通信用暗号鍵を用いてディジタル情報を暗号化及び復号して通信する。



1

【特許請求の範囲】

【請求項1】　秘密鍵暗号方式によりディジタル情報を暗号化して伝送するディジタル通信方法において、
送信側では、
通信の開始時に通信用暗号鍵を自動的に作成し、
該通信用暗号鍵を通信用暗号鍵解読鍵を用いて暗号化し、
該暗号化した通信用暗号鍵を他のディジタル情報に先だって送信し、
受信側では、
暗号化された通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて復号し、
以後、該通信用暗号鍵を用いてディジタル情報を暗号化及び復号して通信するようになしたことを特徴とするディジタル通信方法。

【請求項2】　秘密鍵暗号方式によりディジタル情報を暗号化して送信するディジタル通信装置において、
通信用暗号鍵を暗号化するための通信用暗号鍵解読鍵を記憶する記憶手段と、
通信の開始時に通信用暗号鍵を自動的に作成する通信用暗号鍵作成手段と、
前記通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて暗号化する通信用暗号鍵暗号化手段と、
該暗号化した通信用暗号鍵を他のディジタル情報に先だって送信する送信手段とを備えたことを特徴とするディジタル通信装置。

【請求項3】　秘密鍵暗号方式により暗号化されたディジタル情報を受信するディジタル通信装置において、
通信用暗号鍵を復号するための通信用暗号鍵解読鍵を記憶する記憶手段と、
暗号化された通信用暗号鍵を受信する受信手段と、
該受信した暗号化された通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて復号する通信用暗号鍵復号手段とを備えたことを特徴とするディジタル通信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、テキスト、音声、画像データ等のディジタル情報を暗号化して伝送するディジタル通信方法及びその装置に関するものである。

【０００２】

【従来の技術】従来より、この種の通信方法に使用される暗号方式は種々提案されているが、そのうち１つに秘密鍵暗号方式と呼ばれるものがある。この方式は送信時に任意の秘密の情報（暗号鍵）を用いて暗号化するとともに、受信時に同一の暗号鍵を用いて復号する方式である。秘密鍵暗号方式の暗号化及び復号のアルゴリズムとしては、ＦＥＡＬ（Fast Data Encipherment Algorism:高速データ暗号アルゴリズム）やＤＥＳ（Data Encryption Standard:米国連邦規格の暗号アルゴリズム）等が知られており、これらのアルゴリズム又はアルゴリズムを組込んだＬＳＩを用いることにより、容易に暗号化及び復号を行うことができる。

2

【０００３】前述した秘密鍵暗号方式を用いた従来の通信方法として、センタにより暗号鍵を集中的に管理して通信する方法がある。図２は前述した従来の通信方法による通信のようすを示すもので、図中、１は鍵管理センタ、２は発信端末、３は着信端末である。鍵管理センタ１には、暗号通信を行う端末の各ＩＤ及びこれに対応する通信用暗号鍵解読鍵を予め登録しておくものとする。

【０００４】発信端末２は発信時に鍵管理センタ１へ自分のＩＤ＃ｉ及び着信先のＩＤ＃ｊを送り、通信用暗号鍵Ｋｓを要求する(I)。鍵管理センタ１は発信側のＩＤ＃ｉ及び着信側のＩＤ＃ｊより両端末の通信用暗号鍵解読鍵Ｋｉ，Ｋｊを検索するとともに、通信用暗号鍵Ｋｓを自動的に作成する。次に、鍵管理センタ１は発信側のＩＤ＃ｉ及び通信用暗号鍵Ｋｓを通信用暗号鍵解読鍵Ｋｊで暗号化し、得られたE_{Kj}（Ｋｓ，＃ｉ）に通信用暗号鍵Ｋｓ及び着信側のＩＤ＃ｊを加え、さらに通信用暗号鍵解読鍵Ｋｉで暗号化し、得られたE_{Ki}｛Ｋｓ，＃ｊ，E_{Kj}（Ｋｓ，＃ｉ）｝を発信端末２に送る(II)。

【０００５】発信端末２は送られてきた情報を通信用暗号鍵解読鍵Ｋｉで復号し、得られたＫｓを通信時の暗号鍵として使用するとともに、E_{Kj}（Ｋｓ，＃ｉ）をそのまま着信端末３に送る(III)。着信端末３では送られてきた情報を通信用暗号鍵解読鍵Ｋｊで復号し、得られた通信用暗号鍵Ｋｓ、即ち発信端末２側と同一の暗号鍵により暗号通信を行う(IV)。

【０００６】

【発明が解決しようとする課題】しかしながら、前記方法では鍵管理センタが必要となり、また、発信側は着信側との通信に先立って該鍵管理センタに通信用暗号鍵を要求しなければならず、複雑な操作が必要となる等の問題があった。

【０００７】本発明は前記従来の問題点に鑑み、通信端末同士で通信毎に通信用暗号鍵を変更可能なディジタル通信方法及びその装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】前記目的を達成するため、本発明の請求項１では、秘密鍵暗号方式によりディジタル情報を暗号化して伝送するディジタル通信方法において、送信側では、通信の開始時に通信用暗号鍵を自動的に作成し、該通信用暗号鍵を通信用暗号鍵解読鍵を用いて暗号化し、該暗号化した通信用暗号鍵を他のディジタル情報に先だって送信し、受信側では、暗号化された通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて復号し、以後、該通信用暗号鍵を用いてディジタル情報を暗号化及び復号して通信するようになしたディジタル通信方法を提案する。

【０００９】また、請求項２では、秘密鍵暗号方式によりディジタル情報を暗号化して送信するディジタル通信

装置において、通信用暗号鍵を暗号化するための通信用暗号鍵解読鍵を記憶する記憶手段と、通信の開始時に通信用暗号鍵を自動的に作成する通信用暗号鍵作成手段と、前記通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて暗号化する通信用暗号鍵暗号化手段と、該暗号化した通信用暗号鍵を他のディジタル情報に先だって送信する送信手段とを備えたディジタル通信装置を提案する。

【００１０】また、請求項３では、秘密鍵暗号方式により暗号化されたディジタル情報を受信するディジタル通信装置において、通信用暗号鍵を復号するための通信用暗号鍵解読鍵を記憶する記憶手段と、暗号化された通信用暗号鍵を受信する受信手段と、該受信した暗号化された通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて復号する通信用暗号鍵復号手段とを備えたディジタル通信装置を提案する。

【００１１】

【作用】本発明の請求項１によれば、通信の開始時に、送信側において通信用暗号鍵が自動的に作成され、これが通信用暗号鍵解読鍵によって暗号化された上で他の情報に先だって受信側へ送信され、受信側ではこれが送信側と同一の通信用暗号鍵解読鍵によって復号され、以後、この通信用暗号鍵による暗号通信がなされる。

【００１２】また、請求項２によれば、通信の開始時に、通信用暗号鍵作成手段により通信用暗号鍵が自動的に作成され、通信用暗号鍵暗号化手段により予め記憶手段に記憶された通信用暗号鍵解読鍵を用いて暗号化され、送信手段により他の情報に先だって受信側へ送信される。

【００１３】また、請求項３によれば、受信手段により暗号化された通信用暗号鍵が受信され、これが通信用暗号鍵復号手段により予め記憶手段に記憶された通信用暗号鍵解読鍵を用いて復号される。

【００１４】

【実施例】図１は本発明のディジタル通信装置の一実施例を示すもので、ここでは通話を主目的としたものを示す。図中、１１は送信情報を通信回線に対応した信号に変換して送信したり、通信回線を介して送られてくる信号を受信情報に変換したり、発信や着信のための呼制御信号を送信又は受信するための網インタフェース回路、１２は汎用のＣＰＵ及びＲＯＭ、ＲＡＭ等又は専用のＬＳＩで構成され、暗号鍵を用いて送信情報の暗号化及び受信信号の復号を行うための暗号化／復号回路、１３はディジタル信号をアナログ信号に変換したり、アナログ信号をディジタル信号に変換するコーデック部、１４は送話器から入力された信号や受話器へ出力する信号を増幅する通話回路、１５は各通信毎に異なる通信用暗号鍵を自動的かつランダムに作成する暗号鍵作成部、１６は汎用のＣＰＵ及びＲＯＭ、ＲＡＭ等で構成され、各部を制御する制御回路、１７は通信用暗号鍵を暗号化又は復号する際に使用する通信用暗号鍵解読鍵を記憶するメモリ部、１８は受話器、１９は送話器である。なお、通信用暗号鍵解読鍵を記憶するためのメモリ部１７は容量が少なくて済むので、独立したメモリ部１７を設ける代わりに制御回路１６を構成するメモリの空き空間を使用することも可能である。

【００１５】図３及び図４は発信時及び着信時の動作を示すフローチャートであり、以下、これらに従って本装置の動作を説明する。

【００１６】最初に、発信時の動作を説明する。まず、装置に対してオフフック・ダイヤル押下等により発信操作をする（ステップＳ１）と、制御回路１６は通信用暗号鍵解読鍵をメモリ部１７から読み出し、暗号化／復号回路１２に書き込み（ステップＳ２）、網インタフェース回路１１に発信の指示を行う（ステップＳ３）。着信側の装置が応答し、通話回路１４が接続される（ステップＳ４）と、制御回路１６は通信用暗号鍵の作成を暗号鍵作成部１５に指示する（ステップＳ５）。次に、暗号鍵作成部１５で自動的に作成した通信用暗号鍵を暗号化／復号回路１２において通信用暗号鍵解読鍵を用いて暗号化し（ステップＳ６）、該暗号化した通信用暗号鍵を網インタフェース回路１１を通して通信回線に送出し（ステップＳ７）、通話を開始する（ステップＳ８）。

【００１７】送話器１９から入力された送話信号は通話回路１４で増幅され、コーデック部１３でディジタル信号に変換された後、暗号化／復号回路１２において制御回路１６から書き込まれた通信用暗号鍵を用いて暗号化された後、網インタフェース回路１１を通して通信回線に送出される。一方、網インタフェース回路１１を通して通信回線から受信した受信信号は、暗号化／復号回路１２において制御回路１６から書き込まれた通信用暗号鍵を用いて復号された後、コーデック部１３でアナログ信号に変換され、通話回路１４で増幅され、受話器１８から受話信号として出力される。

【００１８】なお、暗号鍵作成部１５で作成する通信用暗号鍵の作成方法は、各種ランダム関数により乱数を発生させる方法、日付け・時間等を初期値にして一定のアルゴリズムで生成させる方法等がある。また、メモリ部１７に記憶する通信用暗号鍵解読鍵としては通信相手毎に異なるものとしても良く、要は発信側及び受信側で同一のものを誤りなく使用できれば良い。また、図３において、通信用暗号鍵解読鍵書き込み処理（ステップＳ２）は、通話回路接続処理（ステップＳ４）の直後に行っても同一の結果が得られる。

【００１９】次に、着信時の動作を説明する。通信回線から着信がある（ステップＳＰ１）と、制御回路１６は通信用暗号鍵解読鍵をメモリ部１７から読み出し、暗号化／復号回路１２に書き込む（ステップＳＰ２）。オフフック等により着信操作を行って（ステップＳＰ３）、通話回路１４が接続された（ステップＳＰ４）後、網インタフェース回路１１を通して通信回線から通信用暗号

鍵解読鍵によって暗号化された通信用暗号鍵を受信する（ステップＳＰ５）と、暗号化／復号回路１２で通信用暗号鍵解読鍵を用いて復号し（ステップＳＰ６）、該復号した通信用暗号鍵を暗号化／復号回路１２に書き込む（ステップＳＰ７）。そして、通信が開始された後は、前述した発信時の場合と同様に通信を行う（ステップＳＰ８）。なお、図４において、通信用暗号鍵解読鍵書き込み処理（ステップＳＰ２）は、通話回路接続処理（ステップＳＰ４）の直後に行っても同一の結果が得られる。

【００２０】図５は本発明のディジタル通信装置の他の実施例を示すもので、ここではデータ通信を主目的としたものを示す。即ち、図１の実施例において、コーデック部１３及び通話回路１４を、それぞれデータ入出力インタフェース回路２１及びデータ入出力装置２２に置き換えたものである。データ入出力装置２２から入力された送信データはデータ入出力インタフェース回路２１を通り、暗号化／復号回路１２において制御回路１６から書き込まれた通信用暗号鍵を用いて暗号化された後、網インタフェース回路１１を通して通信回線に送出される。一方、網インタフェース回路１１を通して通信回線から受信した受信信号は、暗号化／復号回路１２において制御回路１６から書き込まれた通信用暗号鍵を用いて復号化された後、データ入出力インタフェース回路２１を通り、データ入出力装置２２から受信データとして出力される。なお、その他の構成及び動作は図１の実施例と同様である。

＊【００２１】

【発明の効果】以上説明したように本発明によれば、送信側において通信毎に自動的に通信用暗号鍵を作成し、これを受信側で誤りなく解読することができる、即ち通信用暗号鍵の作成のための鍵管理センタを必要とすることなく、当事者間で通信用暗号鍵を各通信毎に変更することができ、これによって複雑な操作を要することなく、通信の開始時（暗号鍵の送信時）を除いて第三者からの盗聴を困難とすることができ、通信のセキュリティを向上させることができる利点がある。

【図面の簡単な説明】

【図１】本発明のディジタル通信装置の一実施例を示す構成図

【図２】従来の秘密鍵暗号方式を用いた通信方法の説明図

【図３】本発明装置の発信時の動作を示すフローチャート

【図４】本発明装置の着信時の動作を示すフローチャート

【図５】本発明のディジタル通信装置の他の実施例を示す構成図

【符号の説明】

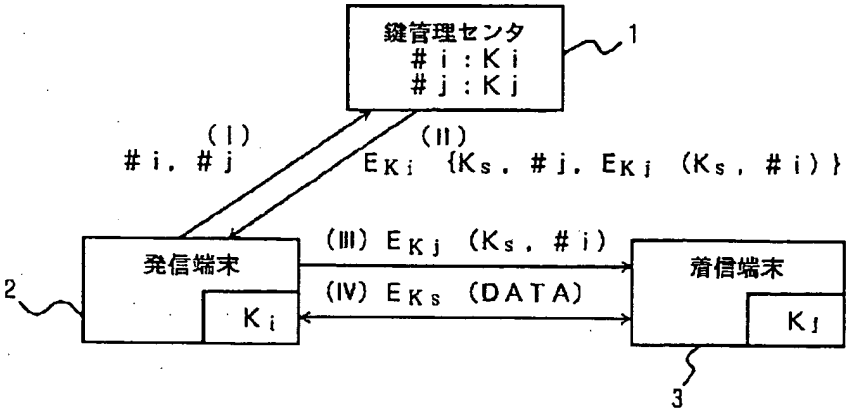
１１…網インタフェース回路、１２…暗号化／復号回路、１３…コーデック部、１４…通話回路、１５…暗号鍵作成部、１６…制御回路、１７…メモリ部、１８…受話器、１９…送話器、２１…データ入出力インタフェース回路、２２…データ入出力装置。

【図２】

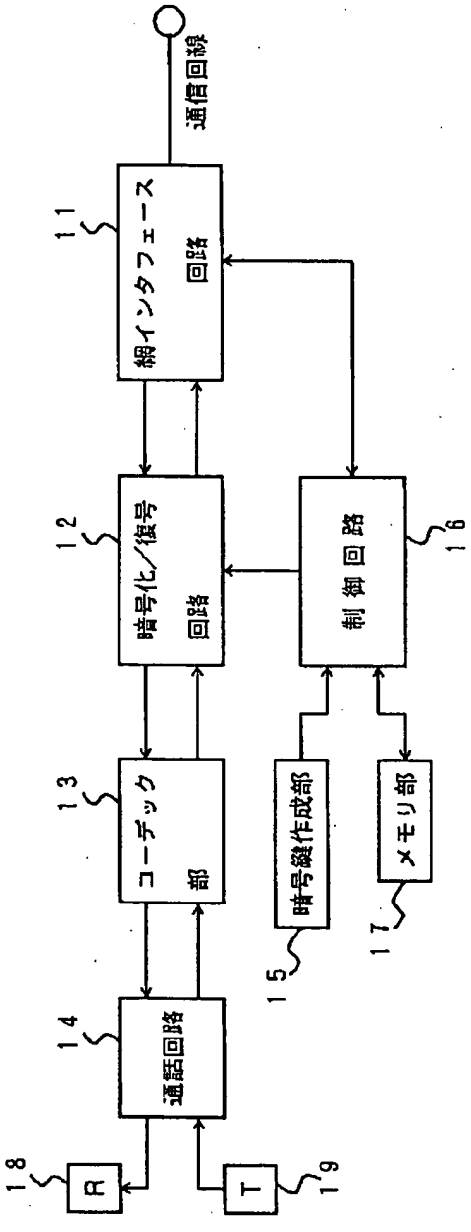
K_s：通信用暗号鍵

K_i，K_j：通信用暗号鍵解読鍵

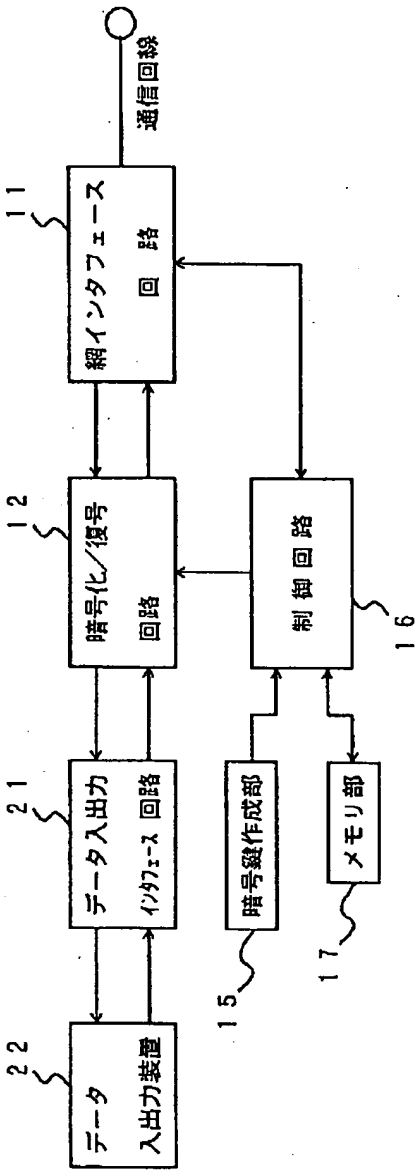
＃i，＃j：発信，着信側ＩＤ



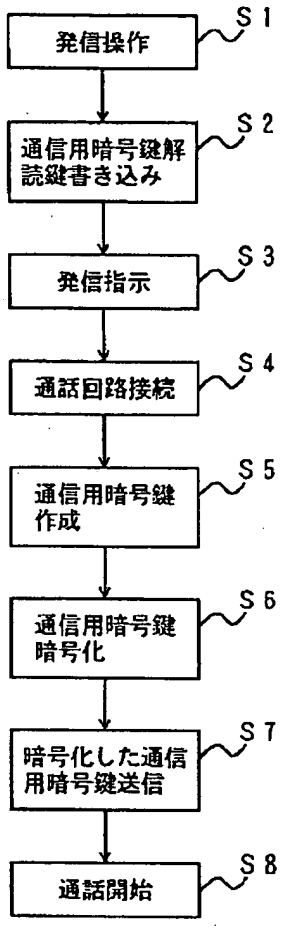
【図1】


通信回線
11
網インタフェース 回路
12
暗号化／復号 回路
13
コーデック 部
14
通話回路
15
暗号鍵作成部
16
制御回路
17
メモリ部
18
R
19
T

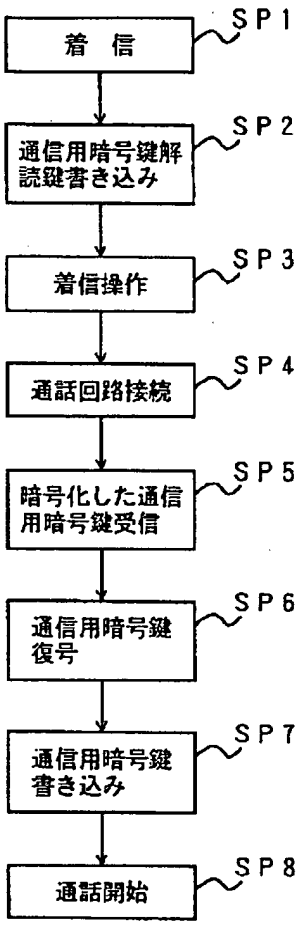
【図5】


通信回線
11
網インタフェース 回路
12
暗号化／復号 回路
21
データ入出力 インタフェース 回路
22
データ 入出力装置
15
暗号鍵作成部
16
制御回路
17
メモリ部

【図3】


発信操作
S1
通信用暗号鍵解読鍵書き込み
S2
発信指示
S3
通話回路接続
S4
通信用暗号鍵作成
S5
通信用暗号鍵暗号化
S6
暗号化した通信用暗号鍵送信
S7
通話開始
S8

【図4】


着　信
SP1
通信用暗号鍵解読鍵書き込み
SP2
着信操作
SP3
通話回路接続
SP4
暗号化した通信用暗号鍵受信
SP5
通信用暗号鍵復号
SP6
通信用暗号鍵書き込み
SP7
通話開始
SP8